3/28/2012

PROVINCE OF BRITISH COLUMBIA
RISK MANAGEMENT BRANCH AND
GOVERNMENT SECURITY OFFICE

RISK MANAGEMENT GUIDELINE FOR THE BC PUBLIC SECTOR

FORWARD

Risk is uncertainty. It is inherent in everything we do. It is what brings both hazards and opportunity to our lives and work. When we wake in the morning and start to plan our daily activities, we instinctively consider the risks along the way; will traffic be heavy, requiring me to leave early for work. Alternatively, will it be light, allowing me to spend a bit more time with the children over breakfast? Routine activities, such as those we encounter daily in life and work, do not need a lot of formal risk management; we have internalized those processes to such an extent that they have become second nature. The potential impacts of risk within the government context, however, are often more severe than being late for work.

Citizens rely on us to provide essential services. They expect well run programs and tax dollars well spent. Government takes on the biggest risks in society and provides critical services where mistakes can cost lives. As a result, a more formal approach to risk management is appropriate.

When examining the risks associated with achieving the goals and objectives of government, it is often prudent to ask first, “How do existing legislation, regulations and current ministry/agency policies and practice guide how we do business?” Numerous policies and controls are in place to manage known risks. Initially, the most effective risk management technique is often compliance with these pre-existing policies and controls.

Next, ask, “What other uncertainties might exist that could have an impact (positive or negative) on my goals and objectives?” Risk management helps answer this question, and provides a process by which anyone can identify and assess the risks; evaluate them; develop prevention, mitigation and recovery strategies; and ultimately achieve their goals most efficiently.

This guideline and the companion *CAN/CSA ISO 31000: Risk Management – Principles and Guidelines* provides the direction and process for standardizing the risk management practice in the Province.

TABLE OF CONTENTS

SECTION 1 – GENERAL

1.1 VISION

Ours is a provincial public sector that accepts risk as an integral part of doing business; manages risk by optimal monitoring, treatment, and transfer; and consciously retains residual risk at an appropriate level.

1.2 SCOPE

This document replaces Risk Management Branch's *Enterprise Risk Management (ERM) Guidelines Version 2.2*, which is hereby withdrawn. Core Policy and Procedures Manual Chapter 14 makes mandatory the establishment and application of risk management across government. This RMB Risk Management Guideline guides the application of risk management within ministries, central agencies and service crowns. Commercial Crowns (such as ICBC, BC Hydro, and BC Transit), and other members of the wider public sector such as health authorities and school districts are encouraged to review this guideline and apply the contents as appropriate.

1.3 AUDIENCE

This guideline serves primarily BC government ministry and provincial public sector employees having risk management responsibilities. It is also a useful reference for those wishing to incorporate the risk management process into business planning, project management, procurement, service delivery and policy development.

1.4 HOW TO USE THIS GUIDELINE

This Risk Management Guideline assists in the application of the provincial risk management standard in public sector settings. The guideline is a companion to:

1. ***CAN/CSA ISO 31000: Risk Management – Principles and Guidelines*** *("the standard"*), is the international standard for risk management. It has been adopted by the government of BC and provides guidance for the provincial risk management framework and process.
2. ***Core Policy and Procedure Manual, Chapter 14*** (*CPPM 14*), provides risk management direction to ministries, Crowns and public sector agencies. It assigns specific risk management roles and responsibilities, establishes the Enterprise Risk Management (ERM) framework and policy throughout the public sector, and details specific risk management and reporting processes and tasks.
3. ***Supporting tools and documents***, such as the Standard Risk Register, Risk Dictionary, Likelihood and Consequences Guide, and guides to loss reporting, insurance, indemnities, and financial guarantees are available at the Risk Management Branch website .

1.5 OBJECTIVES

The provincial risk management objectives are as follows:

a. Senior strategic level decision-making and planning are informed by accurate and congruent assessment of risk across diverse ministries and the wider public sector through formal cross-government Enterprise Risk Management (ERM) framework and processes.

b. Effective Ministry and public sector organization operational decision-making is guided by accurate and congruent assessment of risk within and across diverse business areas. The Risk Management framework and process in place at the ministry or public sector organization level feed into the government-wide ERM framework while meeting the needs of the distinct organizations.

c. Adherence to current risk management principles and best practices across government, making optimum use of established risk management programs, while encouraging a culture that embraces innovation and opportunity, informed risk-taking, and the acknowledgement of risk as inherent in all activities of government.

SECTION 2 – BC RISK MANAGEMENT

2.1 PROVINCIAL RISK MANAGEMENT FRAMEWORK

The BC Government Risk Management Framework consists of the standards, policies, culture, responsibilities, and governance and reporting structures within which the risk management process is applied.

CSA/ISO 31000 defines the risk management process adopted by the government of BC. The application of the risk management process can be viewed on a continuum from the factoring of basic risk information into routine daily business decisions, to the formal conduct of detailed risk assessments as part of government-wide strategic planning. Regardless of scope, the process as explained in detail in section 3 of this guideline remains the same.

Along the continuum of risk management, three basic provincial perspectives emerge. These are Enterprise Risk Management (ERM), ministry and operational risk management, and the delivery of central risk management programs and services.

1. ***Enterprise Risk Management (ERM)****:* ERM describes the integrated and coordinated application of risk management congruently *across* ministries and public sector agencies, and *through* each organization, from cabinet, ministry executive, division, branch and work unit, right down to the individual employee providing front-line service. In this context, *enterprise* implies the whole of government –the full breadth of the BC public sector. A common risk management process applied across government, combined with consistent risk reporting to executive and senior leaders will aid strategic decision-making, planning and resource allocation. ERM allows government leaders to:
    a. Identify risks that are shared across government;
    b. Apply combined risk mitigation strategies;
    c. Determine overarching priorities;
    d. Facilitate discussion of the types and levels of risk government is prepared to accept (tolerance); and
    e. Make long-term plans for the future.

2. ***Ministry and operational level risk management****:* risk management processes and policies applied within ministries (and their constituent divisions, branches, agencies and programs). Ministry and operational risk management is focussed

for the most part internally, to promote the success of internal ministry goals and objectives. Being scalable, the basic risk management process is the same whether employed to inform the ministry's annual business and service plans, or to help inform a daily business decision.

Operational risk management also refers to those areas of specialist risk such as information technology, emergency management, physical security, procurement, and business continuity. These specialist areas of risk, while guided by their own policies and procedures, are an integral part of government's integrated risk management approach. As such, they should be coordinated with the ministry/agency risk management program. Regardless of the ministry or agency applying specialized risk management, common themes and best practices have developed. Additional resources specific to some of these activities are available through ministry experts, or from Risk Management Branch.

3. ***Central risk management programs and services****:* these are the programs and services offered by the Risk Management Branch to address specific risk management needs of government and public sector service providers. Examples include:
    a. risk management consulting and advisory services;
    b. Claims and Litigation Management for some public sector agencies; and
    c. risk financing programs.

For more information on central risk management programs and services, visit Risk Management Branch website at http://gww.fin.gov.bc.ca/gws/pt/rmb/.

2.2 ROLES AND RESPONSIBILITIES

The following roles and responsibilities enable the effective application of risk management throughout government and the wider public sector.

Deputy Ministers are responsible for:

a. ensuring their ministry's compliance with government's risk management policy as established in CPPM Chapter 14.
b. establishing a risk management framework within their ministry and associated Crown corporations and public sector agencies. That framework should complement and support the ERM framework of government;
c. integrating the approved risk management process into existing ministry planning, reporting, operations, and service delivery functions.
d. implementing risk management strategies to address identified risks within their ministry.

Risk Management Branch is responsible for:

a. performing the functions of a government-wide Chief Risk Office;
b. providing central risk management programs, advice and consultation services to all of government and the wider public sector; and
c. operating the Government Security Office, including the role of Chief Security Officer, with overall responsibility for security within government.

Internal Audit and Advisory Services is responsible for:

a. using ERM to inform the annual IAAS risk-based government-wide annual audit work plan;
b. reviewing risk management practices across government; and
c. assessing the effectiveness of established risk mitigation strategies/controls within ministries and across government.

Every manager is responsible for:

a. integrating sound risk management planning and process into the business processes they are responsible for; and
b. reporting risks with causes, impacts, or mitigations beyond their scope of responsibility to executive.

Every employee is responsible for:

a. applying sound risk management within the scope of their duties and responsibilities; and
b. reporting risks with causes, impacts, or mitigations beyond their scope of responsibility or available resources to their manager.

2.3 POLICY

Government core policy (CPPM Ch 14) provides specific direction for risk management from the three perspectives: ERM, ministry and operational risk management, and central risk management programs and services. Consult this chapter regularly to ensure effective risk management development, practice and policy compliance.

2.4 ADDITIONAL INFORMATION

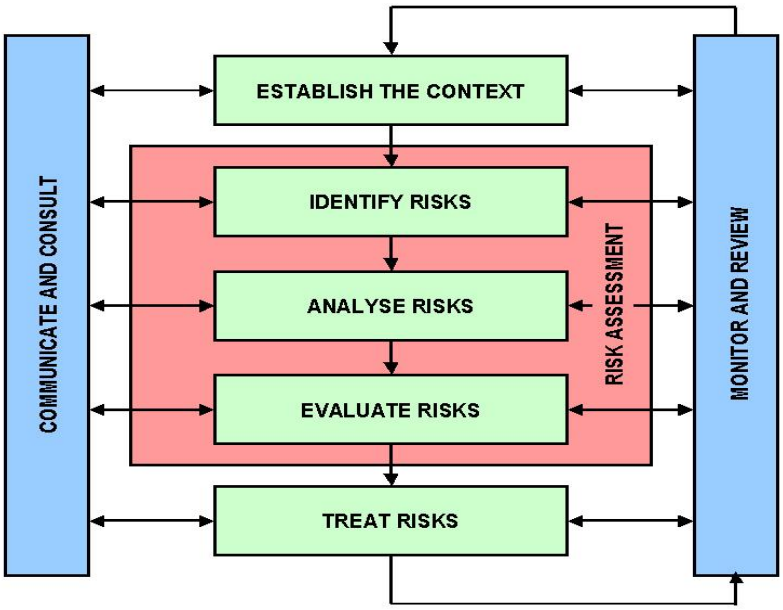
To support the BC public sector, and to provide risk management advice from a government-wide perspective, the Risk Management Branch offers consultation services in areas as diverse as security and loss prevention, insurance, procurement, project management, health and education risk financing programs, and claims and litigation.

For more information, or to engage the services of a Risk Management Consultant, contact Risk Management Branch, 250-356-1794, or email RMB@gov.bc.ca . Tools and references are available on the Risk Management Branch's website at: http://gww.fin.gov.bc.ca/gws/pt/rmb/index.stm .

SECTION 3 – APPLICATION OF RISK MANAGEMENT PROCESS

3.1 GENERAL

CSA/ISO 31000 establishes the provincial risk management standard. It consists of the seven elements in the diagram below and it is scalable. This means it is as applicable to the assessment of risks at the strategic all-of-government level as it is to work unit business planning, project management and daily business decisions. Two elements – *Communicate and Consult*, and *Monitor and Review*, occur continually throughout the process. The remainder are usually undertaken sequentially.



The risk management process should be an integral part of management. It benefits existing business processes by clarifying goals and objectives, identifying what might stand in the way of their achievement, and identifying opportunities to exceed performance objectives, regardless of where in government it is applied. Starting with the strategic goals and objectives of government, carrying on to ministry service and business plans, through division, branch and work unit planning, right down to the performance plans of individual employees, risks can be assessed and mitigated to achieve specific personal, project or program objectives, and ensure alignment with overall ministry and government priorities.

3.2 COMMUNICATE AND CONSULT

> *"Communication and consultation with internal and external stakeholders should take place during all stages of the risk management process" (CAN/ISO 31000, p.14)*

The consultative team approach means that the assessment of risk is proactive and inclusive and involves those who understand the risks and are best able to manage them. Communication and consultation must be used in order to ensure not only that risk reporting goes up to higher levels, but also that executive decisions regarding tolerance of risk and priorities for action get communicated back down to the business unit level.

Depending upon the context, the organization conducting the risk assessment must determine the correct balance of and limits to direct participation. We recognize that it is not always practical or productive to bring all stakeholders to the table. Still, you are seeking a full range of perspective - advocacy, systems, budget, policy, senior leaders, front line delivery and so forth.

Wider participation brings the benefits of greater expertise, experience and buy-in balanced against the requirements for confidentiality, timely action, and strategic scope. RMB can provide advice when deciding which stakeholders should be included in a risk assessment.

3.3 ESTABLISH THE CONTEXT

"Establishing the context" for a risk assessment performs a number of functions. It confirms the subject of the risk assessment, the subject's goals and objectives, and the goals and objectives of the risk assessment itself; identifies stakeholders; and acknowledges constraints and limitations imposed on the project and on the risk management process.

Factors influencing context may be internal, such as executive direction, government policies, budget, regulations and culture; or external, such as other government jurisdictions, national or international economic forces, climate and natural events, or citizens and special interests.

> *"By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process" (ISO 31000, p. 15).*

When applying the risk management process to day-to-day decision making, it may be sufficient to establish the context informally. Formal risk assessments, however, benefit from a formal examination and recording of context. A written document will ensure all stakeholders involved in the process have a clear understanding of the context. It also proves invaluable for recording the environment in which the risk management decisions are made, and can demonstrate due diligence if those decisions are revisited later. For this reason, establish the risk assessment's scope, criteria, and deliverable in writing using the following six headings as a guide:

1. ***Subject of the risk analysis:*** What is being reviewed e.g. is it a strategic plan, service plan, project, program, policy, process or procedure? State the scope with respect to organization, hierarchical level, and time frame. Specify whether the context is strategic or operational.

Hint: If there is no plan or policy yet created, and there is a need for a risk profile on a particular issue, then the subject of the risk analysis may be the status quo i.e. the organization's current approach to the issue. If general goals or values are stated, (see next) the team can generate a risk profile.

***Goals and objectives*:** You should clearly establish what the risk assessment seeks to do because there may be multiple sets of related goals and objectives:

- Those of the ministry, division or branch sponsoring the risk assessment. Clearly establishing those higher goals and objectives will help ensure the subject of the risk assessment is aligned with strategic direction;
- Those of the program, policy or plan in question. Risks are best identified in relation to either broad strategic goals (at the highest level of planning) or in relation to objectives and specific activities. The list of goals, objectives and strategies (activities) can serve to structure the discussion of risk.
- Those of the risk assessment process itself. A risk assessment may inform whether a proposal or project should proceed, or be used to ensure success upon announcement of proposed implementation.

Hint: If there is no program of activities designed yet (see previous comment), state the highest overall goals, and sketch the main components of a draft plan. This will provide a basis to generate a risk profile and mitigations to inform a final plan

2. ***Value criteria:*** These are the guiding principles of the organization, such as a professional ethical code, business practices, political priorities, or operating principles found, for example, in existing vision and mission statements. They might take the form of special rules; e.g., how to conduct business in a specific context. Participants refer to value criteria in order to help to identify and assess risks.

Hint: It is important to keep value criteria in plain view during the session. They serve as a common point of reference to help resolve controversy, and formulate and assess risks.

3. ***Stakeholder analysis:*** This involves the identification of internal and external stakeholders and their respective roles, degree of influence, interests and motives and position with respect to value criteria. They can be both bearers of risk, and/or sources of it.

Hint: Refer to existing consultation papers. A diverse range of session participants, where appropriate and within the limits of facilitation, lends rigour to the process and leads to a better quality result. Tools to assist in the conduct of a stakeholder analysis are available from Risk Management Branch.

4. ***Assumptions and constraints:*** These fixed deadlines, executive directives, resources or other limiting conditions.

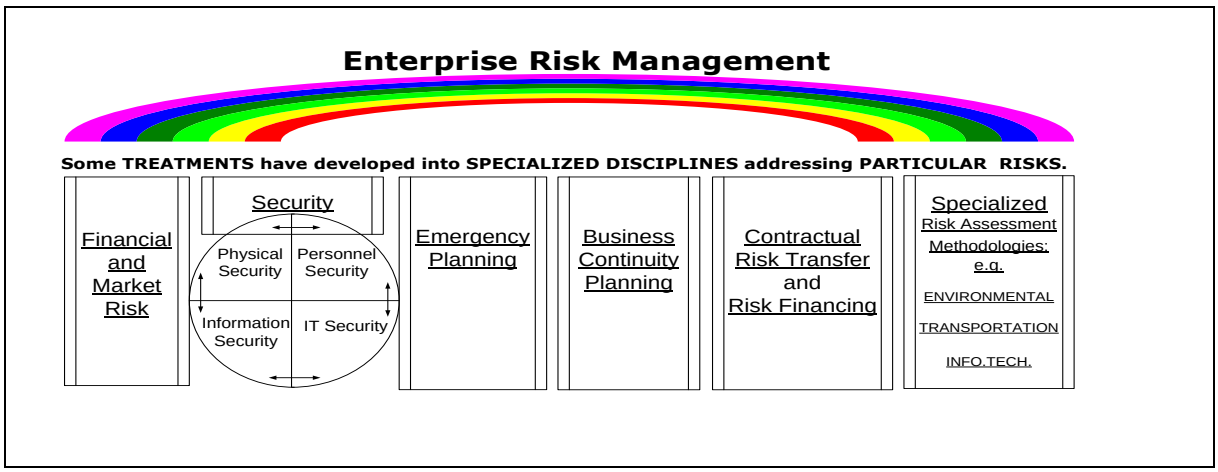
Hint: Legislation, regulation and policy are part of the context in which the risk assessment will take place. Not only do they often address the risks identified, but they also guide the implementation of proposed mitigation strategies.

5. ***Deliverable for the session:*** This is the intended product of the session. A typical deliverable statement might be *"*a comprehensive list of risks, with rankings and summary treatments arrived at by consensus, to inform an improved business plan/policy/program".

3.3.1 Specialized Contexts: Sub-disciplines within Risk Management

Do not let the identification of risk stray out of scope of the defined context. Recognize, too, that certain perils or exposures call for a *specialized risk analysis* as a *separate exercise*. For example, earthquake, hurricane or flood hazards create risk exposures in almost any context. Those risks belong to a specialized analysis for *emergency and business continuity planning*. Similarly, security risks with respect to physical dangers, facilities, and procedures, require a *security review*, which is an expertise unto itself. These specialized areas bring their own criteria and resources to bear upon the process.

Hint: Risk Management Branch can assist with many of these specialized sub-disciplines, and can refer client ministries to other experts across government, such as Emergency Management BC, Government Chief Information Officer, and Treasury Board Staff.



3.4 IDENTIFY RISKS

3.4.1 Risk Identification Methods:

Some basic tools to help in risk identification include surveys, loss histories, process flowcharts, and expert advice within and beyond the organization. Other methods include:

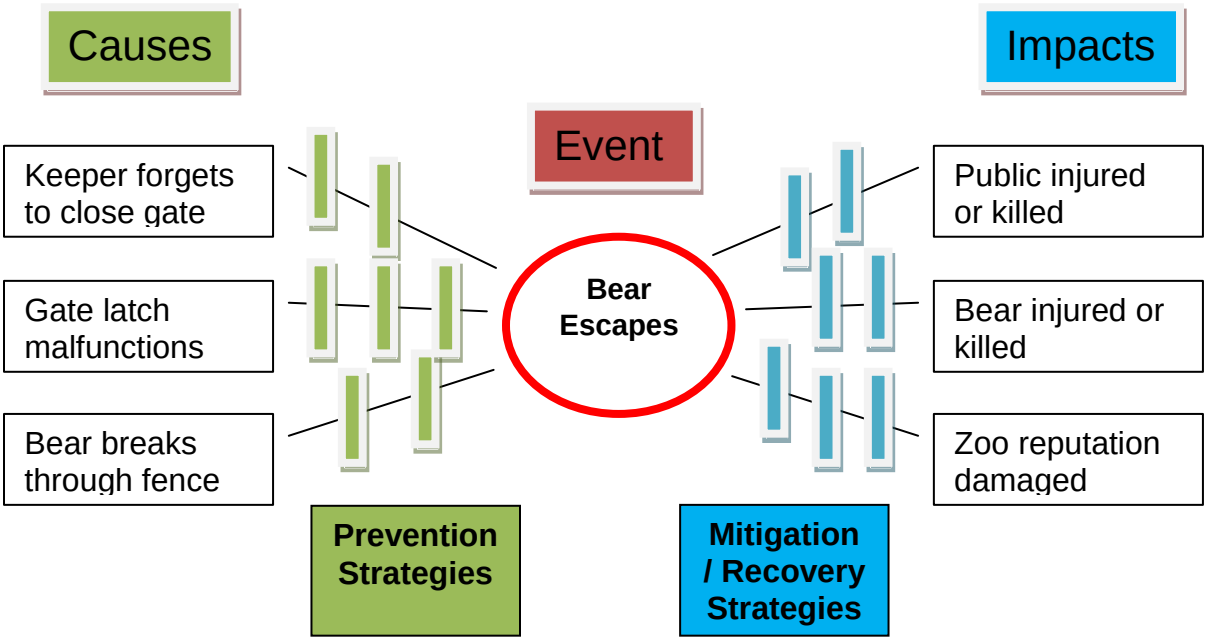
- interview/focus group discussion
- audits or physical inspections
- brainstorming
- questionnaire, Delphi technique
- networking with peers, industry groups and professional associations
- judgemental – speculative, conjectural, intuitive
- history, failure analysis, and loss reports (such as government's General Incident or Loss Reports (GILRs))
- examination of personal experience or past agency experience
- incident, accident and injury investigation
- scenario analysis
- decision trees
- strengths, weaknesses, opportunities, threats (SWOT) analysis
- flow charting, system design review, systems analysis,
- work-breakdown structure analysis

Many ministries and public agencies have designated risk management positions or employees with risk management experience. Consult with internal risk management resources, and inform ministry risk management experts of your risk management activities. In their absence, Risk Management Branch's consultants are trained facilitators and can assist your organization with the risk assessment process.

3.4.2 How to State Risks

The recommended method for stating risk involves considering its three elements: event, causes, and impacts. As with the fire triangle with fuel, oxygen, and a source of ignition, where removal of one element prevents or extinguishes fire, identifying risk by its three elements provides us with three options for treating it. By acting on one of the elements, you can affect the risk.

Since we define risk as "*the effect of uncertainty on objectives*", it is helpful to link your organization's objectives to the risk identification. Define the event as something that could prevent achievement of an objective, milestone or target, or create an opportunity to exceed them. From there, the causes and impacts become easier to identify. Use of a bowtie diagram, as illustrated below, can be helpful in identifying multiple causes and impacts of a single event:



A generic example of a negative risk tied to a goal of a fictitious entity – a zoo. In this case, a strategic organizational objective is *"safe and secure stewardship of their animal exhibits"*. A risk event that could influence that is *"escape of the bear"*. Causes and impacts flow from this event.

1. Identify a risk event related to an in-scope objective. Do not state general unfavourable conditions, in and of themselves, as risk events.

2. List the potential causes of such an event. There are often multiple causes for a given risk event. Ask yourself "why" the event might happen. Use of root cause analysis methods (such as the *Five Whys* tool) can be effective.
3. Identify the impacts of the event, should it happen. Ask yourself, "So what if the event were to occur?" Keep asking "so what" to the chain of impacts until all realistically potential impacts are identified.

Example

Event: Failure to secure project objective #1: Treasury Board approval for required project funding.

Causes:

a. Possible 10% budget cut across government.
b. TB submission fails to link project goals with Ministry objectives.
c. Failure to meet submission deadlines.

Impacts:

a. Possible termination of project.
b. Resubmission to Treasury Board and costly delays.
c. Funding of project from within existing operational budget, leading to service reductions elsewhere.

The *risk register* is the tool that the government uses to document the risk assessment and manage the risk management process. We do not recommend using risk registers pre-populated with generic risks. The list may be inaccurate, incomplete, or poorly stated and participants may not own them. Such lists often stifle the brainstorming process.

3.4.3 Existing Mitigations

Once the risk is clearly identified detailing event, causes and impacts, it is important to identify existing mitigations. Ask what measures are currently in place (if any) to mitigate this risk. List only those mitigations that already exist. Identification of additional proposed mitigations (if required) happens later, after the group has evaluated the adequacy of existing mitigations and the significance of the risk.

3.5 ANALYZE RISK

3.5.1 Risk Rating

Risk analysis is the process of calculating the likelihood of an event and the consequence if it were to occur. The product of these two variables is the *Risk Rating*.

Likelihood: is the chance that the risk event identified will actually occur. When available, statistical data can support estimates of likelihood and severity. In practice, however, often we do not have historical data. Instead, we often rely on the experience of those around the table; therefore, likelihood rarely implies mathematical certainty; rather it is a subjective estimate.

LIKELIHOOD = Probability of the risk event actually occurring.		
SCORE	**DESCRIPTOR**	**HOW LIKELY (%)**
1	Improbable - rare	less than 5
2	Unlikely	5 - 25
3	Possible	25 - 55
4	Likely	55 - 90
5	Almost Certain	90 - 99

Consequence: is the severity of effect upon goals, objectives, or values. A ministry or public sector entity can adjust the consequence criteria appropriate to their lines of business (perhaps quantifiable in terms of budget dollars), and risk appetite. Many organizations develop a "scorecard" with several categories of consequence.

***CONSEQUENCE** = Degree of severity, with respect to goals/values, should the risk event occur.*		
SCORE	**IMPACT**	**DESCRIPTOR**
1	Insignificant	• Negligible effects • STRATEGIC VIEW: NORMAL DIFFICULTIES ASSOCIATED WITH PROGRAM PLANNING AND OPERATIONS
2	Minor	• Normal administrative difficulties • STRATEGIC VIEW: DELAY, IN YEARS, IN FULFILLING THE MANDATE OF THE INSTITUTION]
3	Significant	Delay in accomplishing program or project objectives
4	Major	• Program or project re-design, re-approval and re-do required. Fundamental rework before objective can be met • [STRATEGIC VIEW: STRATEGIC PLAN REQUIRES MAJOR RE-ORIENTATION, APPROVAL; CONSEQUENT PROGRAM RE-WORK]
5	Severe/Catastrophic	• Project or program irrevocably finished; objective will not be met • [STRATEGIC VIEW: MANDATE OF THE ORGANIZATION, OR ORGANIZATION ITSELF AS WE KNOW IT, IS FINISHED]

5	LOW	MEDIUM	HIGH	EXTREME	EXTREME
4	LOW	MEDIUM	HIGH	HIGH	EXTREME
3	LOW	MEDIUM	MEDIUM	HIGH	HIGH
2	LOW	LOW	MEDIUM	MEDIUM	MEDIUM
1	LOW	LOW	LOW	LOW	LOW
LIKELIHOOD	1	2	3	4	5
	CONSEQUENCE				

RANKING L x C Matrix

Score 0-5 = Low
Score 6-10 = Medium
Score 12-16 = High
Score 20-25 = Extreme

3.5.2 Risk Rating Terms

The terms associated with the ranking of risks vary across the risk management discipline; therefore, some clarification is required. *Inherent Risk, Initial Risk, Residual Risk, Current Risk, and Risk Tolerance* are common terms used within the provincial government and the wider public sector. It is not necessary to use all the different risk ratings for any particular risk assessment, but as a minimum, the rating of *initial risk* is required and *residual risk* is recommended.

Inherent risk: involves rating the exposure in the absence of existing controls. When seeking to understand inherent risk, we are considering a hypothetical condition free of all controls, like locks, rules, procedures, ethics and so forth. This can be difficult to imagine. However, there is value in assessing risk this way as it can identify whether an exposure is over- or under-controlled. This is of particular interest to ministry executive and auditors. Strategic risk assessments, of ministry business plans, for example, often benefit from an assessment of inherent risk.

Initial risk: involves rating the exposure within its current control environment (i.e. now). Initial risk is a baseline against which you can measure progress. Reviews of loss histories, reviews of similar sectors' loss histories, and consultation with stakeholders can support the assessment process.

Residual risk: involves rating the exposure after the development of additional mitigation/treatment strategies. It is important to establish a residual risk rating because it is a prediction of the efficacy of proposed mitigations. It also serves as a start point for an informed discussion of acceptable risk with senior decision-makers.

Current risk: is a measure of progress. Later, regular updates on the progress of risk mitigation strategies can be valuable in helping to demonstrate progress or to secure additional resources for stalled mitigation efforts. The tracking of current risk over time allows efficient shifting of resources to problem areas or to areas of opportunity. In addition, tracking the progress of current risk can help demonstrate the effectiveness of the organization's risk management program.

Risk tolerance: is the maximum level of risk the organization is willing to accept for a particular exposure. Executive should provide this once briefed on the nature of the risk, existing controls and the implications of planned mitigations. Ideally, residual risk and risk tolerance are equal. This would confirm that senior executive has committed to the planned additional mitigations and has consciously retained the remaining residual risk.

3.6 EVALUATE RISK: EXISTING CONTROLS, TOLERANCE AND ACTION

Risk evaluation consists of considering the ranked risk in relation to existing controls and the organization's tolerance for the particular risk in question. The purpose is to arrive at a decision as to how to respond to risks – guided by specific value criteria and cost/benefit. There are three considerations when evaluating existing controls. Enter the following into the risk register columns (see *Standard Risk Register*).

1. *Characterize, in qualitative terms, the existing controls* (i.e., How would you describe the process, policy, device, practice or other action already in place that mitigates the risk in question?):

   Non-existent, Inadequate, Adequate, Robust, Excessive (this latter indicates over-controlling and so possibly overspending).

2. *Characterize the risk in relation to the organization's degree of tolerance*:

   Unacceptable/ Acceptable with treatment/ Acceptable

   It is possible to have 'zero" tolerance for certain risks (assuming one can avoid them). A risk may be "Acceptable" either because it is inevitable and too prohibitive to treat, or because it is immaterial and not worthwhile to treat. Over time, ministries may develop risk criteria or measures of risk tolerance or risk thresholds. Expressing tolerance for an unexpected financial loss over a certain percentage of operating budget as "unacceptable" might be one way executive can quantify their tolerance of certain risks.

3. *Decide on consequent action*, based on steps 1) and 2):

   Avoid/ Treat/ Monitor only (tolerate)

   You may avoid a risk altogether, if unacceptable, by not doing the action that would incur it in the first place. We tolerate and monitor risk when treatment is impracticable or prohibitive. We monitor risks that are inconsequential, but whose status might change.

3.7 TREAT RISK

If the current level of risk unacceptable or acceptable with treatment you should recommend a mitigation strategy.

Risk Avoidance: It may be possible to eliminate a risk event entirely by ceasing the activity associated with the event. Given that government delivers society's riskiest services to its most vulnerable members, this is not often possible. It is worth asking though "if this activity is something that government needs to be doing?" Risk *avoidance* is the term given to the elimination of risk by ceasing the associated activity, but it often introduces new risks, especially reputation loss.

Prevention and Mitigation Strategies: Other than avoidance, risk treatments work to prevent the event by addressing the causes, or decrease its impacts by mitigating the negative effects and preparing for post-event recovery. Ask the group "what might be done to prevent the event from happening", then ask, "If it were to happen, how can we limit the damage done and get back to business?"

3.7.1 Diversity of Risk Treatment (Mitigation)

As discussed in section 1, existing legislation, regulation, policies and procedures effectively mitigate many government risks. These legal and administrative controls effectively reduce to tolerable levels most risks associated with routine activities. The first risk management priority of a ministry should therefore be a review of procedural controls and remedial action to educate and encourage compliance. Internal Audit is an excellent resource to assist in assessing compliance with policy.

Should existing treatments be inadequate, the subject be new, or if the context in which it is applied should change, a risk assessment and consideration of additional treatments may be appropriate.

Treatments (risk mitigations) can consist of virtually any sort of administrative action, as well as the application of specialized disciplines – where a separate analysis may be required; e.g., emergency planning, business continuity planning, security planning, risk financing; financial controls; human resources management. Grouping risks in categories can help in the design of cost-effective treatments.

3.7.2 Ensuring Effective Risk Treatment (Mitigation)

In government and public sector work, three points are necessary to underscore:

1. ***Treatments are <u>new</u> measures undertaken to mitigate identified risk***. At times, participants fall into familiar thought patterns and merely repeat the list of existing controls, and say there is nothing more to be done. Alternatively, they may say that the implementation of their planned program activities constitutes mitigation of risk. It is just here where the facilitator or risk champion may add value:
    - A facilitator can lead off by asking (either naïve or well-informed) questions about possible treatments and stimulate discussion;
    - A facilitator can draw attention to the ranking of the risk – if participants are reminded that it is high or extreme, and threatens the viability of the program, they will feel less inclined to leave the matter unattended;
    - A facilitator can introduce categories of implementation risk (well-documented, common reasons for program failure) to inform the analysis;
    - The necessity to study the issue and develop treatments “off-line” or in a separate session can be flagged;
    - The possibility of inviting expertise from outside the immediate group can be raised;
    - At a minimum, the action of documenting the risk and bringing it to the attention of a higher authority or other entity constitutes an improvement in the management of the risk.

2. ***Document treatments*****.** During the latter part of a risk identification and analysis session, make summary statements of treatments. They might have to be elaborated upon elsewhere, but briefly summarizing them allows the facilitator to cover a maximum amount of material. A measure of due diligence is achieved by recording both the risks *and* how they will be managed.
3. ***Translated treatments into action*****.** Suggested treatments (mitigation of either a risk likelihood or degree of consequence) are subject to cost-benefit analysis. The facilitator must challenge the participants to commit to acting upon mitigation strategies. If the risk management initiative is an enhancement to existing processes, then the treatments must become new items in the list of project tasks or business plan strategies. Assigning an individual by name to the development of a mitigation strategy, identifying a specific deliverable, assigning

a due date, and listing required resources all bring value and practicality to the risk assessment, and help transform planned mitigations into action. Risk Management Branch's *Standard Risk Register* is formatted in such a manner, and is an excellent option for ministries initiating the process for the first time.

3.8 MONITOR AND REVIEW

3.8.1 Monitor: Regular Management of Risk Information

Monitoring has to do with managing your risk information as a regular practice. Risks themselves undergo change and can require revision in terms of their description and ranking. New risks appear. Old material requires striking through (~~striking through~~ but not deleting) and archiving. Therefore, we recommend a periodic updating of risk information, using the risk register as a management tool – perhaps as the first agenda item in regular meetings. When used to track the implementation of mitigation strategies and the resultant impact on risk ratings, the risk register becomes a valuable communication tool by informing executive on the progress or lack thereof, and any additional resources required.

A note on risk management software: Initial trials with software designed to assist with the risk management process showed that simple spreadsheets are often more appropriate to support the early proof of concept. Define your processes and information needs. A mature practice of integrated service planning, performance, and risk management may eventually warrant the use of a specialized application, and Risk Management Branch can provide some advice on products that may be available, or attributes that should be included.

3.8.2 Review: Historical Risk Information

In a mature practice of risk management, a growing body of information can inform analysis of the risks themselves, their most common sources, their frequency and impacts /costs of actual occurrence, the efficacy of treatments, and the occurrence of unforeseen events. All of this serves to better manage risks and inform planning. Audits, complaints investigations, legal judgements, and retrospective cost/benefit analysis are some sources of historical risk information.

Another tool that facilitates the collection and analysis of historical information is government's *General Incident or Loss Report (GILR).* The GILR is a reporting tool for a loss, or incident with the potential to lead to a loss. It allows for tracking of property losses and "near misses", identification of trends, and development of treatments. As such, it is one of the tools available to assist in assessing risk.

Use of the GILR is mandated by Core Policy and Procedures Manual (CPPM), Policy 20 (Loss Management) and Procedure L (Loss Reporting). Download a printable GILR form here or from E-forms.

3.9 RECORD THE RISK MANAGEMENT PROCESS

Risk Management documentation includes:

- ***Your organization's policies and framework*** for implementing and guiding the ongoing application of the risk management process. These documents set risk management goals and expectations, establishes the ministry risk management framework, assigns responsibilities and resources, establishes executive's risk

tolerances and appetite, and gives guidance for organization-specific processes, reporting structures, etc. Risk Management Branch can help ministries and the wider public sector develop and implement Risk Management plans.

- ***Your organization's risk assessment documentation***, including context analyses, risk registers complete with treatment strategies, and supporting historical data.

RMB provides help interpreting and implementing these guidelines. Contact the Risk Management Branch at 250-356-1794, or RMB@gov.bc.ca

APPENDIX 1 – ENTERPRISE RISK MANAGEMENT CULTURE: Getting started

Organization's sometimes struggle with enterprise risk management implementation. It is helpful to begin with the view that ERM is an end state. ERM is the outcome of your commitment rather than a process unto itself. It can involve a significant cultural shift which cannot be imposed by edict alone and which takes time to fully mature. The risk maturity self-assessment tool found on this page provides some insight into the practices, policies and tools of a maturing risk management culture.

It is important to recognize the distinction between risk assessments and enterprise risk management:

Where risk assessments are:	Enterprise risk management is:
Narrowly focussed, considering a single program, process or project	Broadly focussed, considering risks across and through the organization
A moment in time	Ongoing and continuous
A tool to focus resources within a project	A tool to redistribute resources across an organization
Shared with immediate team and decision makers	Shared with Executive and senior leadership and informs business planning.
Typically operational in focus	Typically strategic in focus
Managed on a spreadsheet or simple table	Managed via a database for improved reporting
Championed by team or project leads	Championed by Executive and senior leaders

START WITH YOUR BUSINESS PLAN

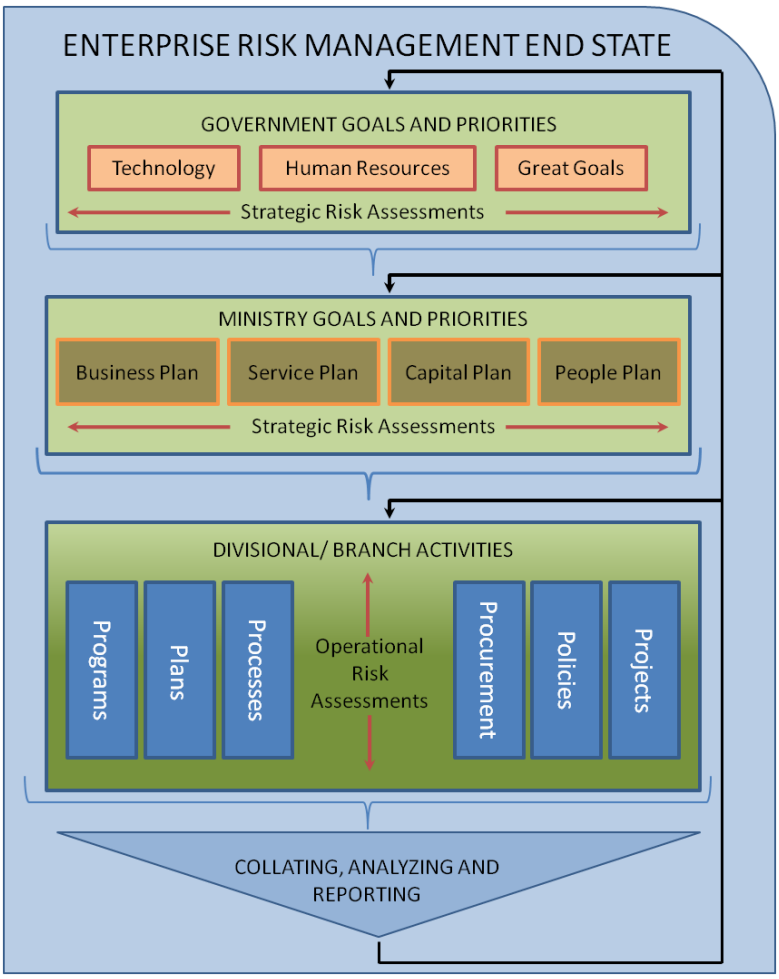
Annual risk assessments are a policy requirement of CPPM Chapter 14. Notwithstanding the policy obligation, this makes an excellent starting point on the path to ERM maturity. An assessment of the overarching strategic risks facing your organization, through a risk assessment of your business plan, is manageable in scope yet corporate-wide in perspective. You will be asking simply, "What could occur that would stand in the way of successfully achieving the goals and objectives of my organization?"

We urge people to keep these processes as simple as possible. Many business solutions founder under the weight of complex and time-consuming steps where the effort is greater than the return. We find facilitated sessions with working groups to be most effective and efficient at producing high quality value-added risk assessments. A representative and knowledgeable working group will understand the organization's operations, its limitations and constraints, and its operating environment. This group can speak to its culture, infrastructure, policies, processes, programs and its people.

If you are new to the risk management process, this link will provide you with more information on the ISO 31000 Risk Management standard and associated guidelines and templates. The same process applies regardless of the scope or type of risk assessment.

A risk assessment to identify, analyze and prioritize key business risks is a tool to guide the execution of your business plan and inform subsequent planning. As you would with

your business planning and performance management activities, we suggest biannual or quarterly reviews of the risk register to monitor for changes to the risk environment and to update mitigation activities.



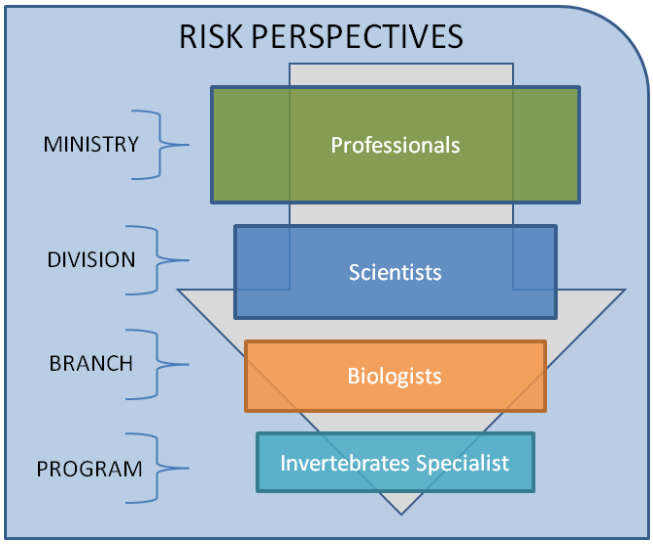
This strategic risk assessment is a critical first step on the road to a more mature risk focused organizational culture. From here, you can push risk management activities downward through the organization. Representative working groups can assess risks facing divisions and branches. They can review programs, processes, policies and projects.

FROM STRATEGIC TO OPERATIONS

As you press down through the organization, the information gathered becomes more granular and uncovers distinct causes and impacts. For example, at a ministry or divisional level your group may indentify the threat of an aging workforce. At a program level, a group may identify the potential loss of a specific skill set or of an individual with specialized knowledge. To mitigate these risks, at the program level you may respond by addressing the specific issue through job sharing or other knowledge management activities. At the enterprise level, you may respond by rolling out a strategic HR plan aimed at ministry-wide hiring policy and retention management.

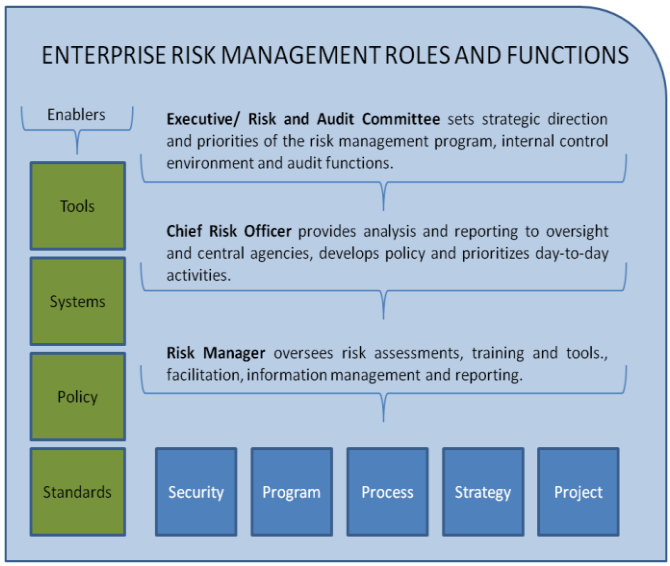
ROLLING IT UP

Another step in the maturity spectrum is collation of individual risk assessments. Essentially, you are gathering disparate and separate assessments and using them to complete a comprehensive catalogue of an organization's strengths and vulnerabilities. This collation and analysis provides a snapshot of the organization, identifying potential causes and impacts, which could stand in the way of successfully meeting goals and objectives. This identification of common causes may help support a business case for a new corporate system, prioritize resources or defend decisions. Over time, through various iterations and planning cycles, these snapshots form a panorama illustrating change over time and trends and ongoing issues. It should demonstrate the effectiveness of your risk mitigation activities and it should help reduce the frequency and severity of negative events. In a maturing ERM culture, executive and senior leaders provide direction on priorities through a consideration of government and organizational priorities and tolerance for different risks.



ERM ROLES AND FUNCTIONS

There is not a prescriptive, one-size-fits- all ERM organizational structure. These structural decisions depend on the size of the organization, the nature of its risks, its culture and risk tolerance and available organizational resources.



There are some essential functional requirements. All ERM regimes need a common repository for risk information, they require analysis and reporting, and they benefit greatly from a champion with good facilitation skills and ability to help build capacity. These functions could be the aegis of one staff member, a dedicated team, or shared more informally throughout the organization. Moreover, ERM requires direction and active engagement from senior leaders.